SPYWOLF

Security Audit Report

Completed on

October 23, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **NYX Soulmate** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

NYX Soulmate

PROJECT DESCRIPTION

According to their whitepaper:

NYX Soulmate is an AI that introduces compatible people in web3.
The current landscape of web2 socialization apps for dating, networking and friendship strongly rely on looks (photo-based inventories). The metaverse won't be about selfies, but avatars. Imagine a room with 250 avatars, who do you approach first? NYX Soulmate facilitates this navigation by providing a layer of intel and introducing people based on who they are, not how they look. It uses a proprietary Ai created by project's team, based on decades of scientific research in psychometrics and Jungian theory.

Release Date: Public mint starts in October, 2022

Category: NFT

CONTRACT INFO

Token Name
Teste

Symbol
TST

Contract Address
0x26313c5d346A646D3dD66F621F6227B60EB610c9

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Oct 20, 2022

Verified?
Yes

Total Supply
7

Status
Launched

TAXES

Buy Tax
none

Sell Tax
none

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of Oct 22, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxTxAmount

Additional information

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	7
Uniq Senders	1
Uniq Receivers	1
Total Amount	7 TST
Median Transfer Amount	1 TST
Average Transfer Amount	1 TST
First transfer date	2022-10-21
Last transfer date	2022-10-21
Days token transferred	1

SMART CONTRACT STATS

Calls Count	12
External calls	12
Internal calls	0
Transactions count	12
Uniq Callers	1
Days contract called	2
Last transaction time	2022-10-21 10:23:43 UTC
Created	2022-10-20 16:08:00 UTC
Create TX	0x983c832e87e63c5a9f7b106191ece0e748ba30aa27ac7572f3de8b42c2093d82
Creator	0x8f8d92a38060b1ffb054b52a3f5ac8dd1156fb6a

FEATURED WALLETS

Owner address	0x8f8d92a38060b1ffb054b52a3f5ac8dd1156fb6a

TOP 3 UNLOCKED WALLETS

1 7 Same as owner

2 N/A

3 N/A

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

Informational

Owner can change vault address.

```
function setVault(address _vault) external onlyOwner {
    vault = _vault;
}
```

Owner can withdraw ETH from contract to vault address.

```
function withdraw() external payable onlyOwner {
    require(vault != address(0), 'Vault Invalid');
    require(payable(vault).send(address(this).balance));
}
```

Owner can set genesis NFT and lite NFT price.

```
function setPrice(uint256 _price) external onlyOwner {
    price = _price;
}

function setLitePrice(uint256 _litePrice) external onlyOwner {
    litePrice = _litePrice;
}
```

Informational

Owner can set max mints per wallet.

```
function setMaxMint(uint256 _maxMint) external onlyOwner {
    maxMint = _maxMint;
}
```

Owner can set allowlist mint price.

```
function setAllowlistPrice(uint256 _allowlistPrice) external onlyOwner {
    allowlistPrice = _allowlistPrice;
}
```

Owner can enable/disable allow list minting.

```
function setAllowlistMintActive(bool _isAllowlistMintActive) external onlyOwner {
    isAllowlistMintActive = _isAllowlistMintActive;
}
```

Owner can add address who can mint with allowlistMint function.

```
function setMerkleRoot(bytes32 _merkleRoot) public onlyOwner {
    merkleRoot = _merkleRoot;
}

function allowlistMint(bytes32[] calldata _merkleProof) nonReentrant payable external {
.........
    bytes32 leaf = keccak256(abi.encodePacked(_msgSender()));
    require(MerkleProof.verify(_merkleProof, merkleRoot, leaf), 'Invalid proof!');
.........

}
```

Informational

Owner can change max genesis and lite NFTs supply.

```
function setMaxSupply(uint256 _maxSupply) external onlyOwner {
    maxSupply = _maxSupply;
}

function setMaxLiteSupply(uint256 _maxLiteSupply) external onlyOwner {
    maxLiteSupply = _maxLiteSupply;
}
```

Owner can enable/disable genesis and lite NFTs minting.

```
function setMintActive(bool _isMintActive) external onlyOwner {
    isMintActive = _isMintActive;
}

function setLiteMintActive(bool _isLiteMintActive) external onlyOwner {
    isLiteMintActive = _isLiteMintActive;
}
```

Owner can add address who can mint free NFT with allowlistFreeMint function.

```
function setFreeMerkleRoot(bytes32 _freeMerkleRoot) public onlyOwner {
    freeMerkleRoot = _freeMerkleRoot;
}

function allowlistFreeMint(bytes32[] calldata _merkleProof) nonReentrant external {
..........
    bytes32 leaf = keccak256(abi.encodePacked(_msgSender()));
    require(MerkleProof.verify(_merkleProof, freeMerkleRoot, leaf), 'Invalid proof!');
..........
}
```

Informational

Owner can restrict NFT transfers

```
function setTransferFreeControl(bool _transferFreeControl) external onlyOwner {
    transferFreeControl = _transferFreeControl;
}

function setTransferControl(bool _transferControl) external onlyOwner {
    transferControl = _transferControl;
}

function _transfer(
    address from,
    address to,
    uint256 tokenId
) internal virtual {
        require(ERC721.ownerOf(tokenId) == from, "ERC721: transfer from incorrect owner");
        require(to != address(0), "ERC721: transfer to the zero address");

        _beforeTokenTransfer(from, to, tokenId);
        ............
}

function _beforeTokenTransfer(address from, address to, uint256 tokenId) internal override(ERC721, ERC721Enumerable){
    if(transferControl == true){
      require(from == address(0) || to == address(0), "Not allowed to transfer your Soul");
      super._beforeTokenTransfer(from, to, tokenId);
    } else if(transferFreeControl == true && freeClaimed[_msgSender()] == true){
        require(from == address(0) || to == address(0) || balanceOf(_msgSender()) > 1,
        "Not allowed to transfer your free Soul");
        super._beforeTokenTransfer(from, to, tokenId);
      } else {
          super._beforeTokenTransfer(from, to, tokenId);
        }
}
```

Informational

Owner can mint new genesis and lite NFTs.

```
function genesisMultiMint(address[] memory _multipleReceiver) public onlyOwner{
    require(totalSupply() + _multipleReceiver.length <= maxSupply, 'Max supply exceeded!');

    for(uint256 i = 0; i < _multipleReceiver.length ; i++){
      freeMintedNFTs++;
      uint256 tokenId = _tokenIdCounter.current();
      _tokenIdCounter.increment();
      _safeMint(_multipleReceiver[i], tokenId);
    }
}

function liteMultiMint(address[] memory _multipleReceiver) public onlyOwner{
    require(_liteTokenIdCounter.liteCurrent() + _multipleReceiver.length <= maxLiteSupply, 'Max supply exceeded!');

    for(uint256 i = 0; i < _multipleReceiver.length ; i++){
      uint256 liteTokenId = _liteTokenIdCounter.liteCurrent();
      _liteTokenIdCounter.liteIncrement();
      _safeMint(_multipleReceiver[i], liteTokenId + 10000);
    }
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

NYX Soulmate

GOOD PRACTICES FOUND

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website

No information found

WEBSITE

Website URL
https://www.nyxsoul.ai/

Domain Registry
https://1api.net/

Domain Expiration

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

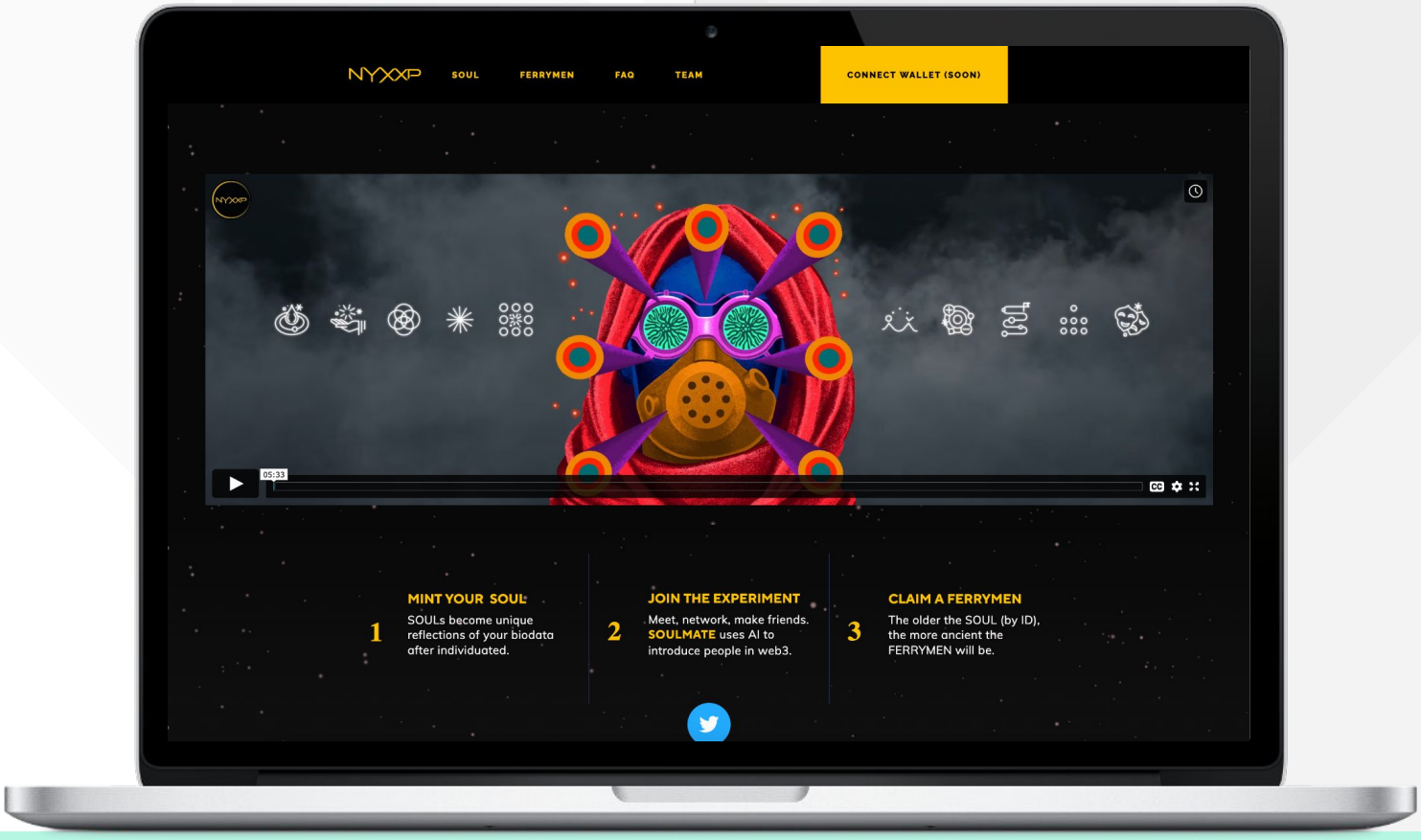
Design
Single page design, nice overall layout, appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found..

Whitepaper
Well written but a bit short

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes



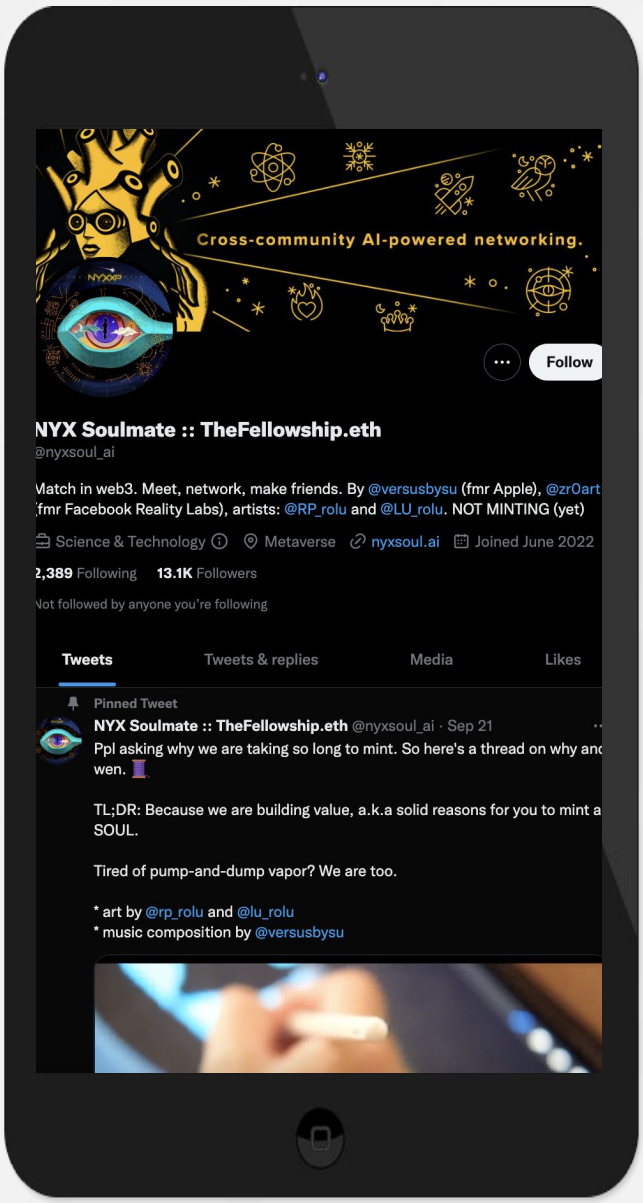
nyxsoul.xyz

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media activity is concentrated in twitter. It consists of organic users interactions.



Twitter

@nyxsoul_ai

- 13 100 followers
- Posts frequently
- Organic users engagement

- Not available

Discord

- The Fellowship, project's custom discord, will open after mint for holders.

- Not available

Telegram

- Not available

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.